SafeNet Authentication Service AD FS Agent

Configuration Guide

Document Information

Document Part Number	007-012546-001, Rev B
Release Date	2 February 2015

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Preface

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	

CHAPTER 1
Introduction

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**
  A cloud authentication service of SafeNet, Inc.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**
  The software used to build a SafeNet authentication service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**
  A term used to describe the implementation of SAS-SPE on-premises.

Environment

Supported Platforms	Windows Server 2012 R2
Supported Architecture	64-bit
Additional Software Components	Microsoft .Net Framework 4.5 Microsoft PowerShell v3.0

Overview

Microsoft introduced multi-factor authentication (MFA) as part of Conditional Access policies in AD FS2. Multi-factor authentication is one of the key elements of conditional access policies in AD FS in Windows Server 2012 R2. Multi-factor authentication has traditionally meant using a smart card or other second factor with AD-based authentication, such as Integrated Authentication. This type of MFA can impose client-side requirements, such as smart card drivers, USB ports, or other client hardware or software that cannot always be expected with BYOD client devices. Because of this, AD FS introduces a new pluggable MFA concept focused on flexibility, integration with AD FS policy, and a consistent user experience.

New Authentication Concepts in AD FS in Windows Server 2012 R2

Primary and Secondary Authentication

Previous versions of AD FS have supported authenticating users against Active Directory using any of the following methods:

- Integrated windows authentication
- Username and password
- Client certificate (client TLS, including smart card authentication)

The above methods are still supported in Windows Server 2012 R2, but are now called “primary authentication” because Microsoft has introduced a new feature called secondary, or “additional”, authentication. This is where SafeNet AD FS Agent, a multi-factor authentication plugin, comes in.

Secondary authentication occurs immediately after primary authentication and authenticates the same AD user. Once primary authentication is complete and successful, AD FS invokes what we call the external authentication handler. This handler invokes an additional authentication provider, either an in-box AD FS provider or an external MFA provider, based on protocol inputs and policy. AD FS passes the primary authenticated user’s identity to the additional authentication provider, which performs the authentication and hands the result back. At this point, AD FS continues executing the authentication/authorization policy and issues the token accordingly.

Authentication Flow

AD FS provides extensible multi-factor authentication through the concept of “additional authentication providers” that are invoked during secondary authentication. External providers can be registered in AD FS. Once a provider is registered with AD FS, it is invoked from the AD FS authentication code via specific interfaces and methods that the provider implements and that AD FS calls. Because it provides a bridge between AD FS and an external authentication provider, the external authentication provider is also called an AD FS MFA “adapter”.

Invoking MFA

There are two ways to configure AD FS in Windows Server 2012 R2 to invoke multi factor authentication—policy configuration or via the WS-Federation or SAML protocol token request.

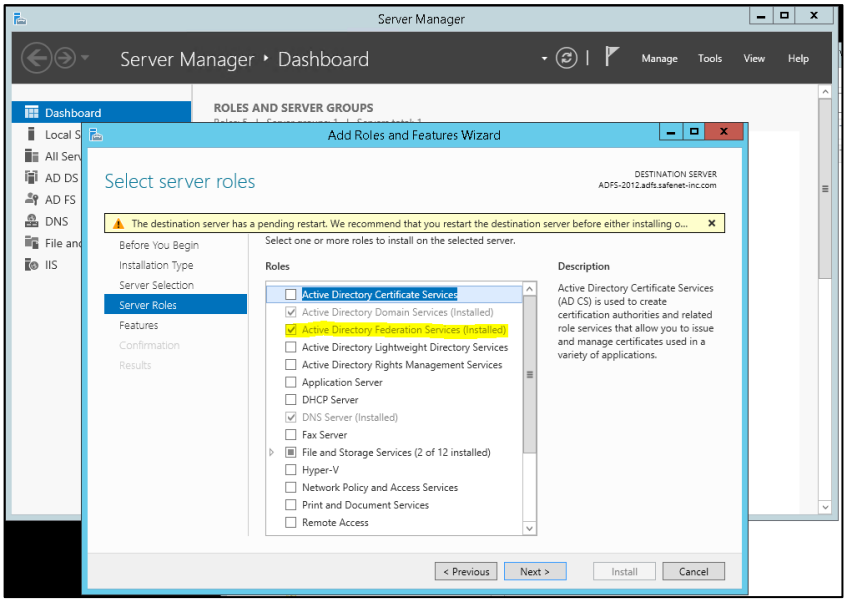
Via policy, AD FS in Windows Server 2012 R2 introduces a new rule set called “additional authentication rules” that are used for triggering multi factor authentication. As with many other settings in AD FS, you can set these rules at a global level or at the relying party trust level.

As part of the new rule set, AD FS introduces a new claim type and value to refer to multi factor authentication. When this claim type and value is generated via an additional authentication rule, AD FS will invoke the external authentication handler, and hence the provider(s) configured on the system. If more than one provider is enabled in AD FS, the user will see a method choice page that presents the friendly name of each provider and allows the user to select one by clicking on it.

Prerequisite Tasks

The following prerequisite tasks must be completed:

- In Windows Server 2012 R2, enable AD FS2.



- Install Microsoft .Net Framework 4.5.
- Install Microsoft PowerShell v 3.0 (available from C:\Program Files (x86)\Reference Assemblies\Microsoft\WindowsPowerShell\3.0).

CHAPTER 2
Installation

Installing the SAS AD FS Agent

To install the SAS AD FS Agent:

1. Locate and run the SafeNet Authentication Service installer:

   SafeNetAuthentication Service Agent for ADFS.exe

2. On the **Welcome** window, click **Next**.
3. On the **License Agreement** window, select **I accept the terms in the license agreement**, and then click **Next**.
4. On the **Customer Information** window, enter **User Name** and **Organization**, and then click **Next**.
5. On the **Destination Folder** window, do one of the following.
   - To select the default installation destination folder, click **Next**.
   - To select a different location, click **Change**, and browse to the appropriate location.
6. On the **Ready to Install the Program** window, click **Install.**

   When the installation process is completed, the **Installshield Wizard Completed** window is displayed.
7. Click **Finish** to exit the installation wizard**.**

CHAPTER 3
Configuring SAS AD FS Agent

Introduction

The Management UI for the agent handles almost all functions except adding new locales. The interface is simple and matches all other agent UIs. It controls the agent registration and deregistration via use of Microsoft PowerShell (v3) API. The agent finds its current launch path and calculates all other paths accordingly. On "Apply", all the current valid paths are saved in the INI file. The series of pictures below show all the available options.

Configuring the SafeNet Authentication Service Manager

To configure SafeNet Authentication Service for AD FS:

1. In the SafeNet Authentication Service Manager, select **Virtual Servers > COMMS > Auth Nodes**.
2. Click **Add**.
3. Enter the IP address of the AD FS agent computer.
4. Click **Apply**.

Configuring the Agent Key File

This agent uses an encrypted key file to communicate with the authentication web service. This ensures all communication attempts made against the web service are from valid recognized agents. To accomplish this, a key file is loaded and registered with SAS agents, and then a matching key file is installed and registered with the web service.

A sample key file (Agent.bsidkey) has been installed for evaluation purposes; however, we strongly recommend that you generate your own key file for a production environment, as the sample file is publicly distributed.

To load the key file:

1. In SAS, select the **COMMs** tab and download an agent key file from the **Authentication Agent Setting**s section.
2. To open the AD FS Agent Manager, select **Start > All Programs > SafeNet > Agents > ADFS Agent**.
3. Click the **Communications** tab.
4. Click the **Agent Encryption Key File** browse button and navigate to the agent key file.
5. Click **Apply**.

Configuring the SAS AD FS Agent

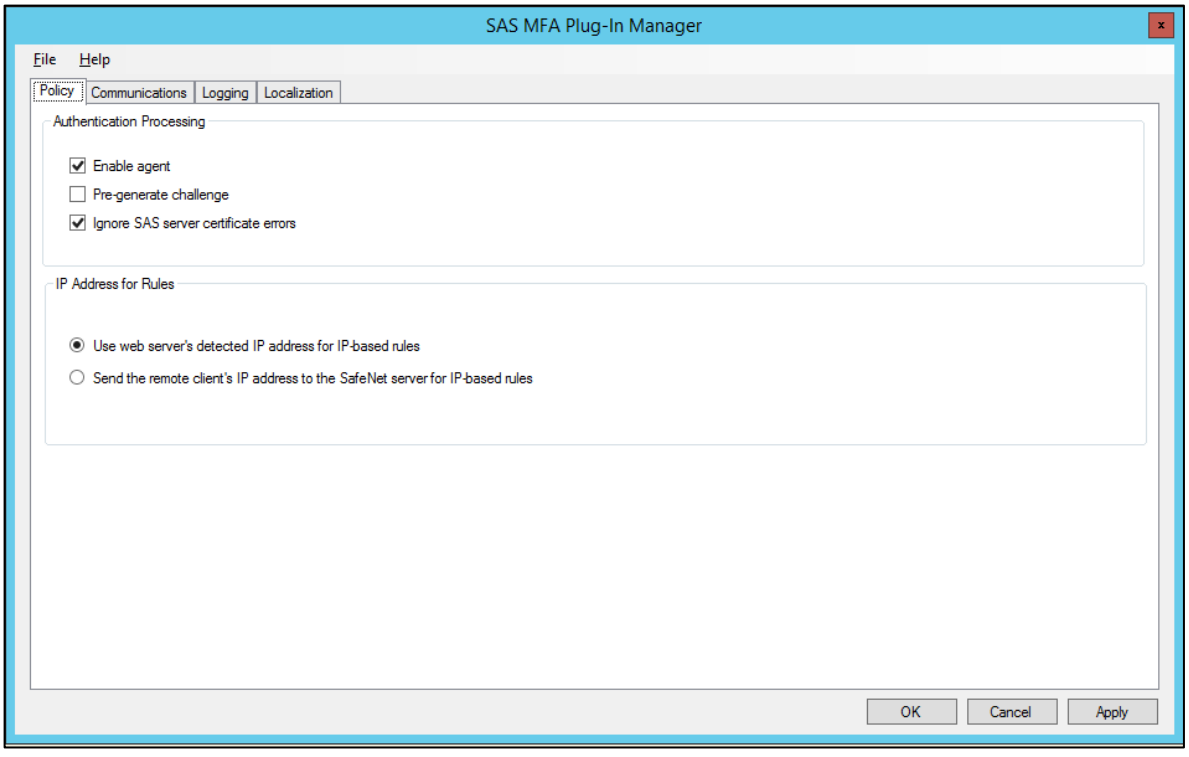
To configure the SAS AD FS Agent:

1. Select **Start > All Programs > SafeNet > Agents > ADFS Agent**.

> **NOTE**: Ensure that the %HOMEDRIVE% of the user being used to run the agent management console is the same as the %WINDIR% root drive. This is required to locate the .Net Global Assembly Cache.
>
> To verify that the two attributes are identical run the following in the command line console using the same user credentials:
>
> echo %HOMEDRIVE%
>
> echo %WINDIR%

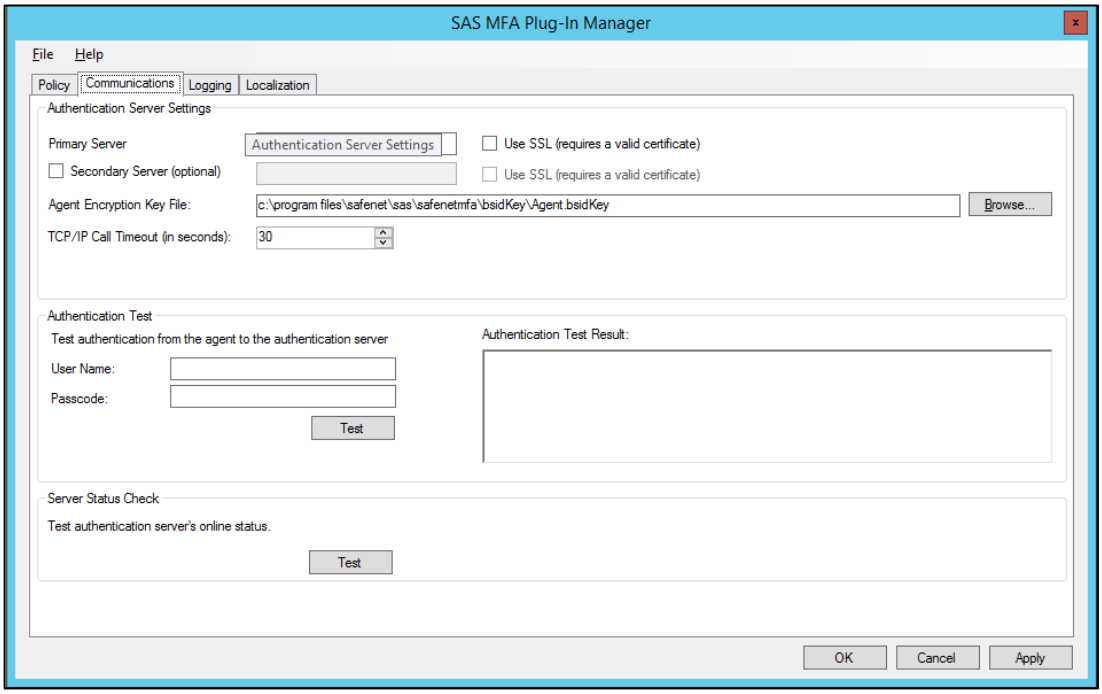
2. On the **SAS MFA Plug-In Manager** window, click the **Policy** tab. Complete the fields as follows, and then click **Apply**.

Enable/Disable Agent	Select this option to enable the SAS AD FS Agent.
Pre-Generate Challenge	Select this option to display the grid immediately following the first authentication step.
Ignore SAS Server certificate errors	Select this option if required to send the remote client's IP address to the SAS Server.

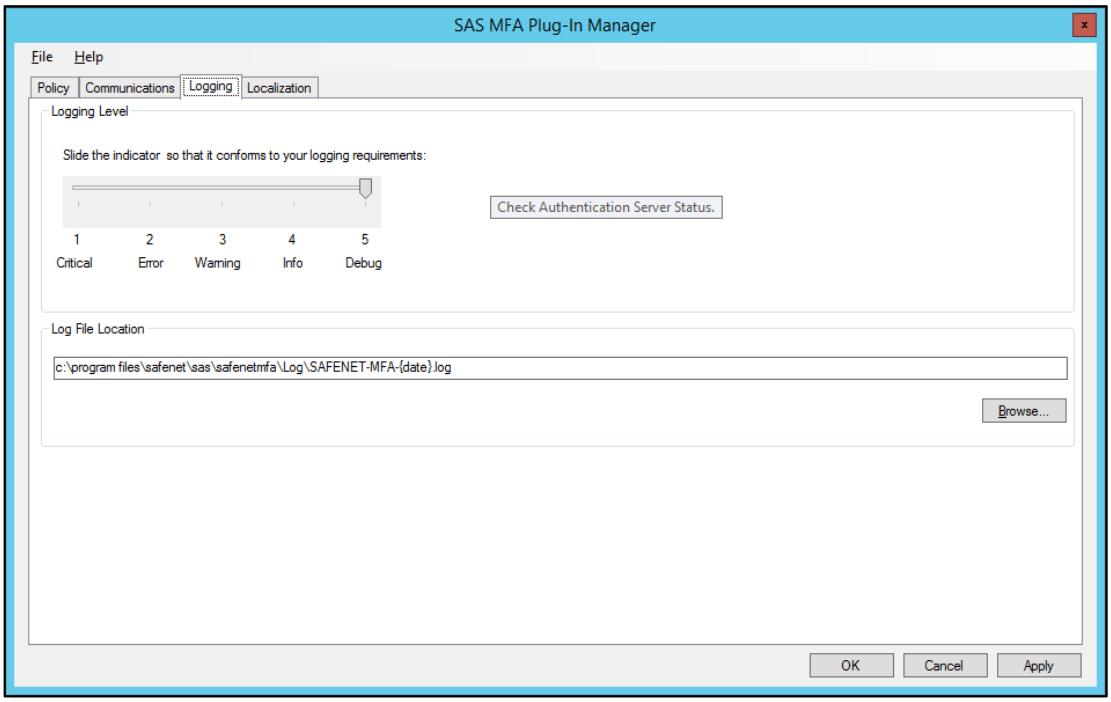


3. Click the **Communications** tab. Complete the fields as follows, and then click **Apply**:

Primary Server (IP:Port)	Enter the IP address of the SAS server.
Agent Encryption File Key	For details, see “Configuring the Agent Key File”, on page 9.



4. Click the **Logging** tab. Select the required logging level and log file location, and then click **Apply**.



Configuring Localization

Localization is controlled by the INI file, which is preconfigured for English-US and French-Canadian.

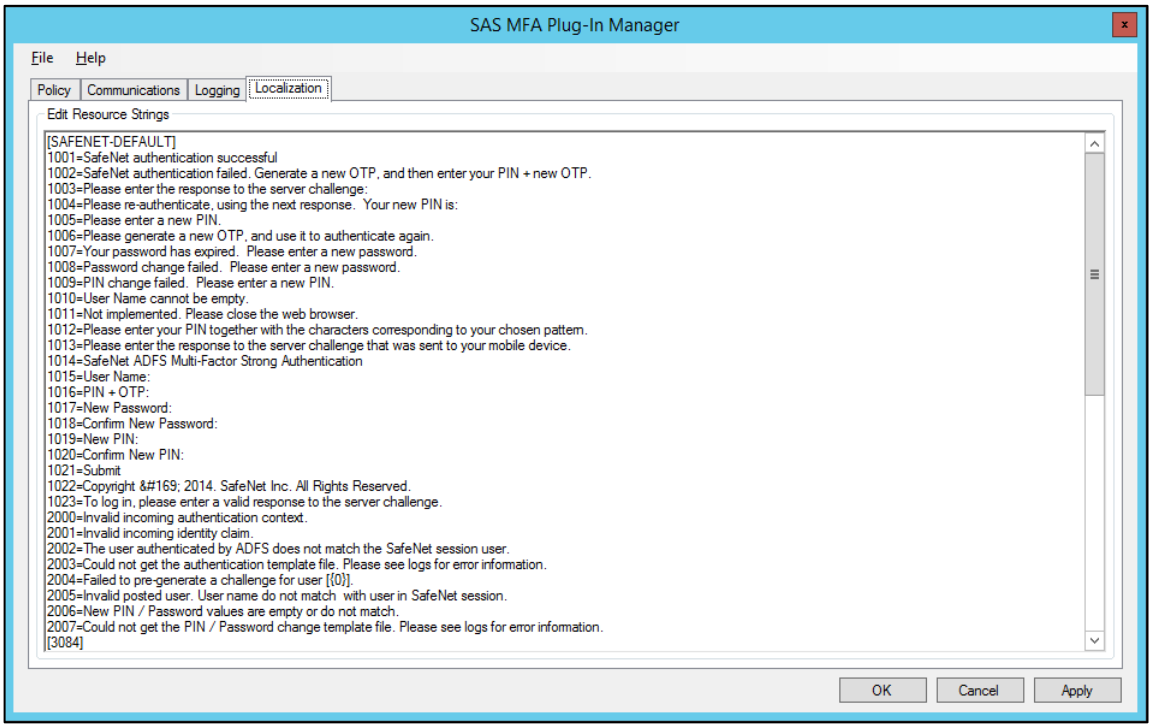
> **NOTE:** The French-Canadian text is for demonstration purposes only. The translation should be proofed by a professional translator before use.

The INI file describes the available options for setting additional localizations. Adding a new localization to the INI file is a manual procedure and rules mentioned in the INI file should be strictly observed.

Extra care must be observed when changing any value in the INI file.

To view the localization settings in the SAS AD FS Agent Manager:

1. To open the AD FS Agent Manager, click **Start > All Programs > SafeNet > Agents > ADFS Agent**.
2. On the **SAS MFA Plug-In Manager** window, click the **Localization** tab.



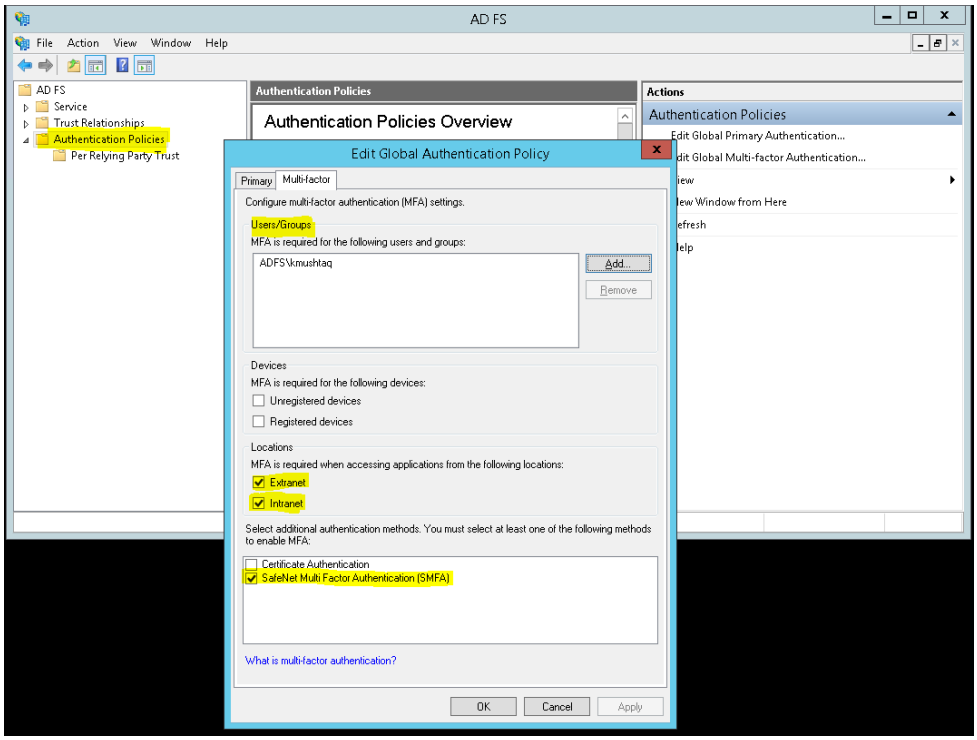
Setting Multi-Factor Policies in AD FS

Enabling the agent on the SAS AD FS **Agent Policy** tab (see “Configuring the SAS AD FS Agent” on page 10 (registers the SafeNet AD FS Agent with AD FS and enables it at global policy level.

After registration, you can enforce multi-factor authentication (MFA) policies at the required level in the **AD FS Management** window.

To enforce MFA policies:

1. In AD FS, select **Authentication Policies**.
2. Select **Edit Global Authentication Policies**.
3. On the **Edit Global Authentication Policy** window, add the required users and groups.



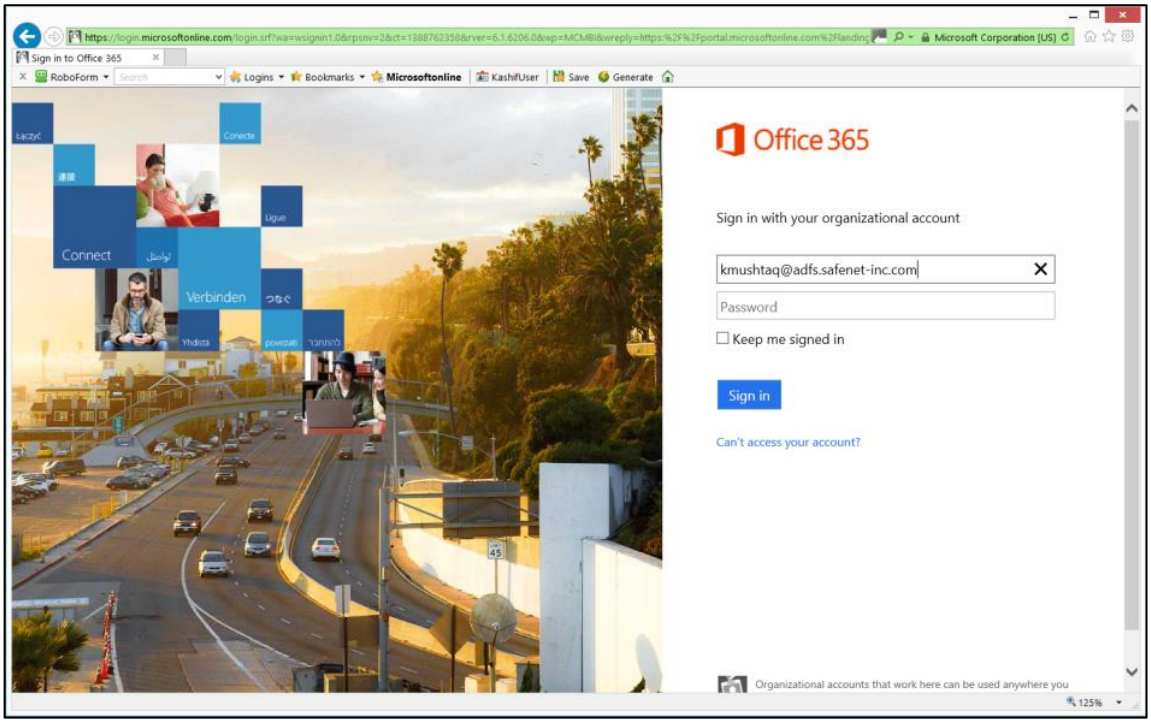
4. Select **Extranet** and/or **Intranet** to specify that MFA is required at these locations.
5. Select the **SafeNet Multi Factor Authentication (SMFA)** method.

CHAPTER 4
Working with Microsoft Office 365

Ensure that you have registered for the Microsoft Office 365 service and promoted your domain to a federated domain.

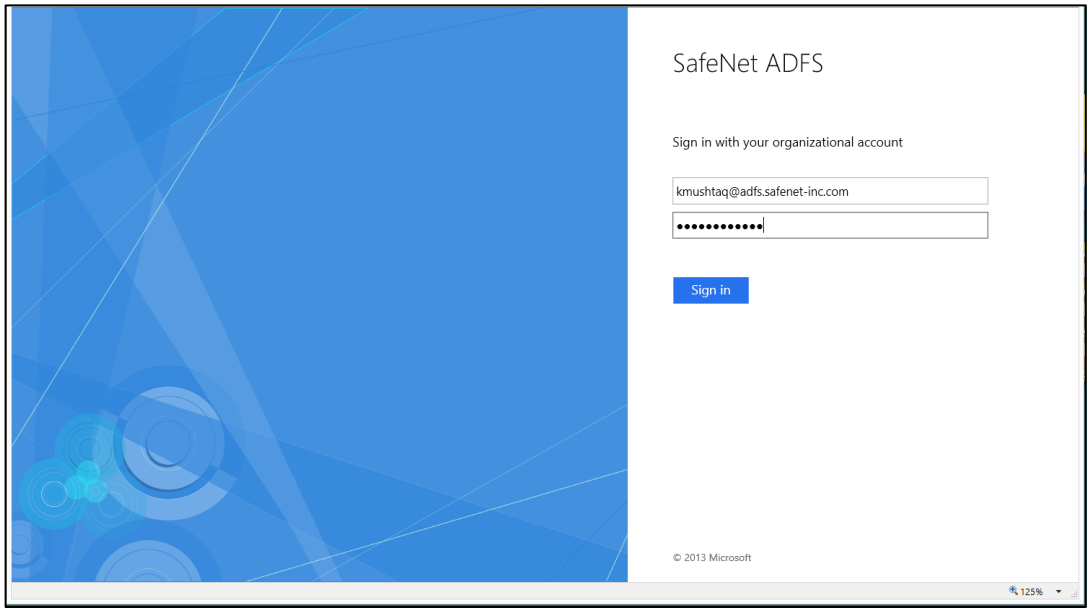
Logging On to Microsoft Office 365

1. Launch **AD FS Manager**.
2. Enable the agent and then enable **Forms Authentication** as the **Primary Authentication** method.
3. Force MFA at the **Extranet** or **Internet** level.
4. Force MFA at the Global or Individual SP level.
5. Open a browser and log in to https://portal.microsoftonline.com/.



Sign-In Window Examples

Primary Authentication (Windows Credentials)



Secondary Authentication (SafeNet Grid Token)